(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－164937
（P2002－164937A）
(43)公開日　平成14年６月７日(2002.6.7)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード*（参考）
Ｈ０４Ｌ　12/66		Ｈ０４Ｌ　11/20	Ｂ	５Ｋ０３０
12/56			１０２Ａ	５Ｋ０３４
29/06			１０２Ｄ	
		13/00	３０５Ｂ	

審査請求　未請求　請求項の数10　ＯＬ　（全 21 頁）

(21)出願番号　特願2000－359296(P2000－359296)

(22)出願日　平成12年11月27日(2000.11.27)

特許法第64条第２項ただし書の規定により図面第２図，５図，６図，８図，９図，10図，11図，12図，15図，23図の一部は不掲載とした。

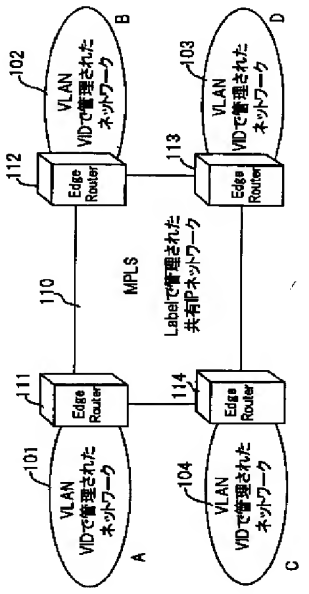
(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(72)発明者　濱　大介
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(74)代理人　100084711
弁理士　斉藤　千幹

Ｆターム(参考)　5K030 GA19 HA08 HC01 HD03 HD07
KA05 KA13 LB05 MD07
5K034 AA14 BB06 DD03 EE11 HH01
HH02 HH14 HH63

(54)【発明の名称】　ネットワーク及びエッジルータ

(57)【要約】
【課題】　VLANでアクセス系ネットワークを構築し、MPLS網でコアネットワークを構築するようにして安価な値段で且つスケール性の高いマルチプロトコルな襖2VPNを提供する。
【解決手段】　共有ネットワーク上にVPNを形成し、該VPN内で通信を行うネットワークにおいて、MPLS網110でVPNのコア網を形成すると共に、VLAN 101～104で該コア網に対するアクセス網を形成し、MPLS網とVLAN間に、これらMPLS網とVLAN間のインタフェース機能を実行するエッジルータ111～114を設ける。送信側のエッジルータはVLANから入力するパケットをMPLSのパケットに変換してMPLS網に送出し、受信側のエッジルータはMPLS網より受信したMPLSのパケットをVLANのパケットに変換し、該VLANパケットを送信側VLANと同一のVPNに属する VLANに向けて送信する。

本発明のVLANとMPLSの混在ネットワークの概略図



【特許請求の範囲】
【請求項１】　共有ネットワーク上にVPNを形成し、該VPNを介して通信を行うネットワークにおいて、
ラベルスイッチ網でVPNのコア網を形成すると共に、VLANで該コア網に対するアクセス網を形成し、
ラベルスイッチ網とVLAN間のインタフェース機能を実行する装置をこれらラベルスイッチ網の端に設けた、
ことを特徴とするネットワーク。
【請求項２】　前記インタフェース装置は、ラベルスイッチ網であるMPLS網の端に設けられたエッジルータであり、
送信側のエッジルータはVLANから送出されるパケットをMPLSのパケットに変換してMPLS網に送出し、受信側のエッジルータはMPLS網より受信したMPLSのパケットをVLANのパケットに変換し、該VLANパケットを送信側VLANと同一のVPNに属する VLANに向けて送信する、
ことを特徴とする請求項１記載のネットワーク。
【請求項３】　前記エッジルータはVLANのパケットに含まれるVLAN識別子(VID)とMPLSのパケットに含まれるVPNラベルの対応を記憶するテーブルを備え、
送信側エッジルータはVLANパケットのVIDに応じたVPNラベルを求め、該VPNラベルを有するMPLSパケットを生成してMPLS網に送出し、
受信側エッジルータはMPLS網より受信したMPLSパケットに含まれるVPNラベルに応じたVIDを求め、該VIDを有するVLANパケットを生成し、該VIDが示すVLANに送出する、
ことを特徴とする請求項２記載のネットワーク。
【請求項４】　前記エッジルータは、受信側のエッジルータに向けてMPLSパケットを送出する経路を決定するルート決定部、ルート決定部により決定された経路を特定する転送用ラベルを受信側エッジルータのアドレスに対応させて記憶するテーブルを備え、
送信側エッジルータは、パケットの宛先MACアドレスに応じた受信エッジルータを求め、該テーブルより受信エッジルータに応じた転送用ラベルを求め、前記VPNラベル及び転送用ラベルを含むMPLSパケットを生成してMPLS網に送出する、
ことを特徴とする請求項３記載のネットワーク。
【請求項５】　前記VPNを構成するVLANに接続するエッジルータはそれぞれ、該エッジルータに接続するVLAN構成装置のアドレスとエッジルータのアドレスを組にして前記他のエッジルータに送出し、各エッジルータは受信情報に基づいてレイヤ2ルーチングテーブルを作成し、
送信側エッジルータは、該レイヤ2ルーチングテーブルより前記パケットの宛先に応じた受信エッジルータを求める、
ことを特徴とする請求項４記載のネットワーク。
【請求項６】　共有ネットワーク上にVPNを形成し、MPLS網で該VPNのコア網を形成し、VLANで該コア網に対するアクセス網を形成するネットワークにおけるエッジルータにおいて、
VLAN識別子(VID)とVPN識別子であるVPNラベルの対応を記憶する手段、
前記対応関係を用いてVLANから送出されるパケットに含まれるVIDに応じたVPNラベルを求め、該VPNラベルを含むMPLSパケットを生成してMPLS網に送出するMPLSパケット生成部、
を備えたことを特徴とする送信側エッジルータ。
【請求項７】　前記エッジルータは更に、受信側のエッジルータに向けてMPLSパケットを送出する経路を決定するルート決定部、
ルート決定部により決定された経路を特定する転送用ラベルを受信側エッジルータに対応させて記憶する転送用ラベル記憶部、
を備え、前記MPLSパケット生成部は、
パケットの宛先MACアドレスに応じた受信エッジルータを求め、該転送用ラベル記憶部より受信エッジルータに応じた転送用ラベルを求め、前記VPNラベル及び転送用ラベルを含むMPLSパケットを生成する、
ことを特徴とする請求項６記載のエッジルータ。
【請求項８】　前記MPLSパケット生成部は、
前記VPNを構成する他のVLANに接続するエッジルータより送られてくる該エッジルータのアドレスと該エッジルータに接続するVLAN構成装置のアドレスとの組み合わせ情報に基づいてレイヤ2ルーチングテーブルを作成し、
該レイヤ2ルーチングテーブルよりパケットの宛先に応じた前記受信エッジルータを求める、
ことを特徴とする請求項７記載のエッジルータ。
【請求項９】　共有ネットワーク上にVPNを形成し、MPLS網で該VPNのコア網を形成し、VLANで該コア網に対するアクセス網を形成するネットワークにおけるエッジルータにおいて、
VLAN識別子(VID)とVPN識別子であるVPNラベルの対応を記憶するテーブル、
前記テーブルを用いてMPLS網より入力するパケットに含まれるVPNラベルに応じたVIDを求め、該VIDを含むVLANパケットを生成してMPLS網に送出するVLANパケット生成部、
を備えたことを特徴とする受信側のエッジルータ。
【請求項１０】　共有ネットワーク上にVPNを形成し、MPLS網で該VPNのコア網を形成し、VLANで該コア網に対するアクセス網を形成するネットワークにおけるエッジルータにおいて、
VLAN識別子(VID)とVPN識別子であるVPNラベルの対応を記憶するテーブル、
前記テーブルを用いてVLANより入力するパケットに含まれるVIDに応じたVPNラベルを求め、該VPNラベルを含むMPLSパケットを生成してMPLS網に送出するMPLSパケット生成部、

前記テーブルを用いてMPLS網より入力するパケットに含まれるVPNラベルに応じたVIDを求め、該VIDを含むVLANパケットを生成してMPLS網に送出するVLANパケット生成部、
を備えたことを特徴とするエッジルータ。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明はネットワーク及びエッジルータに係わり、特に、共有ネットワーク上にVPN(Virtual Private Network)を形成し、該VPN内で通信を行うネットワーク及び共有ネットワーク上にVPNを形成し、ラベルスイッチ網で該VPNのコア網を形成し、VLAN(Virtual LAN)で該コア網に対するアクセス網を形成するネットワークにおけるエッジルータに関する。
【０００２】
【従来の技術】社内のネットワーク（イントラネット）を構築するためには、各地に散在する本社、営業所、支店、工場、研究所等を相互に接続する必要がある。又、本格的な国際化の時代を迎え、イントラネットは日本国内だけで閉じないで、広く海外拠点まで接続する必要性が生じている。このようにイントラネットが広域化すると、離れたオフィスにいてもあたかも本社のオフィスにいるのと同じようなシステム環境を実現する要求が生じ、VPN(Virtual Private Network)技術が開発され広く採用されている。VPNとは共有ネットワーク(インターネット等の広域網)上に設けられ、ユーザが共有ネットワークの利用を意識することなく利用できる仮想の私設網であり、アクセスサーバ、WANルータ、VPN専用装置等を利用してWAN上に構築される。VPNを構築する技術には、IEEE802.1QのVLAN(Virtual LAN)による方法、IPsecによる方法、MPLS(Multiprotocol label Switching)による方法などがある。
【０００３】VLAN(仮想LAN)は、ネットワークに接続された機器をその物理的な配線や構成に関係なくグループ化するもので、グループ化はレイヤ2にあたるMACフレームが到達する範囲内において行われる。フレームの送受は同一グループ内で行われ、フレームのブロードキャストも同一グループ内で行われる。異なるVLANグループ間の通信はレイヤ3における中継動作を行うルータを介さなければならない。VLANを実現する方式には、(1) ポートベースVLAN、(2) MACアドレスデータベースVLAN、(3) ポリシーベースVLANなどがある。このうち、ポートベースVLANは、スイッチングハブ(switching HUB)上の物理ポート単位で静的にVLANグループを形成する方式であり、又、MACアドレスデータベースは端末が持つMACアドレスをベースにしてVLANグループを形成するもので、受信パケット内の発信元MACアドレスに基づいて該当するVLANグループを認識する。
【０００４】図１８はポートベースVLANの構成例であり、スイッチングハブSHBの複数LANポートP1～P6にそれぞれパソコン等の端末が接続されている。LANポートP1～P3はグループ1に属し、LANポートP3～P6はグループ2に属する。グループ1の所定端末から送信されたブロードキャストフレームはグループ1内の端末のみにブロードキャストされ、グループ2の端末から送信されたブロードキャストフレームはグループ2内の端末のみにブロードキャストされる。又、フレームの送受は同一グループ内で行われ、異なるVLANグループ１，２間の通信は図示しないルータを介さなければならない。以上より、グループ化以前にはブロードキャストフレームを全端末に中継していたのがグループ内のみに中継するだけで良くなり、ネットワークの負荷を軽減できる。しかも、他のグループにフレームは送信されないためセキュリティを維持することができる効果が発生する。
【０００５】VLANではLANポートP3のように複数のグループに属するように重複して設定することができる。又、グループ化は１台のスイッチングハブに限らず、図１９に示すように複数のスイッチングハブSHB1～SHB3に属するポートをグループ化することもできる。すなわち、各スイッチングハブSHB1～SHB3のポートP1～P3をグループ化し、各グループに固有の識別子であるVLAN ID(VID:Virtual LAN Identifier)を付与すると共に後述するタグ方式を採用することにより複数の装置にまたがった複数のVLAN(VLAN1～VLAN3)を構成することができる。これにより、同一のVLANに属する端末は設置場所に依存することなく、あたかも同一の物理ネットワークに接続しているかのように通信することができる。
【０００６】ここでタグ方式とは、IEEE802.1Qにより標準化された手法である。タグ方式では、VIDをMACフレームにタグという形で付与し、このタグをパケットと共にMACフレームで運ぶ。タグ付きMACフレームを受信したL2スイッチ(スイッチングハブ)はタグの内容を解析し、そのVLANが属する適切なポートに中継処理する。
【０００７】図２０はVLAN(IEEE802.1Q)のMACフレームフォーマットであり、M1はMAC宛先アドレス(MAC DA)、M2はMAC発信元アドレス(MAC SA)、M3はタグ、M4はタイプ、M5はIPパケット(IPヘッダ/TCPヘッダ/データ部)である。タグM3は４バイトで構成され、①TPID(Tag Protocol Identifier)、②ユーザプライオリティ、③CFI(Canonical Fotmat Indicator)、④VID(Vitual LAN Identifier)、⑤length、⑥RIF(Routing Information Field)を有している。TPIDの値は16進数で81-00(IEEE802.1Qタグタイプ)に固定されている。ユーザプライオリティはフレームの優先順位を3ビットで表現したもの、CFIはタグヘッダにおけるRIF fieldの有無を示すもの、VIDは12ビット構成のバーチャルLAN識別子であり、2^{12}=4096個のVIDを指定することができる。
【０００８】図２１はVLANの実現例であり、PC1～PC4はパソコン端末、SHB1はポートP1、P2にパソコン端末PC1、PC2が接続された第1のスイッチングハブ、SHB2はポ

ートP1、P2にパソコン端末PC3、PC4が接続された第2のスイッチングハブ、SHB3はポートP1、P2に第1、第2のスイッチングハブSHB1,2が接続された第3のスイッチングハブ、RTは第3のスイッチングハブSHB3のポートP3に接続されたルータである。第1、第2のスイッチングハブSHB1,2はそれぞれポートP3を介して第3のスイッチングハブSHB3と接続している。

【０００９】第1、第3のパソコン端末PC1,PC3はVID=10の第1のVLANを構成し、第2、第4のパソコン端末PC2,PC4はVID=20第2のVLANを構成し、又、スイッチングハブSHB1～SHB3の各ポートP1～P3は図中のVID値で示すようにグループ化されている。尚、2つのVID値を有するポートは2つのグループに属するものである。パソコン端末PC1からパソコン端末PC3にパケットを送信する場合、パソコン端末PC1はヘッダにパソコン端末PC3のMACアドレスを宛先アドレスとして有するパケットを送出する。該パケットをポート1より受信した第1スイッチングハブSHB1は、該ポート1の属する VLANのVID(=10)を予め設定されているテーブルより求め、該VID=10を含むタグを受信パケットに付加してVID=10のポートP3より送出する。以後、該タグ付きパケットは第3スイッチングハブSHB3のポートP1,P2を介して第2スイッチングハブSHB2に送信される。第2スイッチングハブSHB2はタグ付きパケットが到来すれば、タグを外してVI=10のポートP1よりパソコン端末PC3に送信する。

【００１０】一方、パソコン端末PC1から別グループのパソコン端末PC4にパケットを送信する場合、パソコン端末PC1はレイヤ2ヘッダにルータRTのMACアドレス(レイヤ2アドレス)を宛先アドレスとして有し、レイヤ3ヘッダ(IPヘッダ)にパソコン端末PC4のレイヤ3アドレス(IPアドレス)を有するパケットをを送出する。該パケットをポート1より受信した第1スイッチングハブSHB1は、該ポート1の属する VLANのVID(=10)をテーブルより求め、該VID=10を含むタグを受信パケットに付加してVID=10のポートP3より送出する。第3スイッチングハブSHB3は該受信パケットをそのままVID= 10を有するポートP3より送出する。ルータRTはパケットを受信すれば、宛先のレイヤ3アドレスを参照してVID値を10から20に変更し、かつ、パケットの宛先MACアドレスをパソコン端末PC4のMACアドレスに変更して該パケットをポートP1より送出する。以後、該タグ付きパケットは第3スイッチングハブSHB3のポートP3,P2を介して第2スイッチングハブSHB2に送信される。第2スイッチングハブSHB2はタグ付きパケットが到来すれば、タグを外してVID=20のポートP2よりパソコン端末PC4に送信する。以上のVLANによれば、企業の情報システム（イントラネット）の既存資産を保存しながら、次世代LANへの基盤を柔軟に構築でき、ネットワーク管理/運用を統合して合理化を図ることができる。

【００１１】VPNを構成する方法としてMPLS(Multiprotocol label Switcing)による方法がある。MPLSは、コネクションという概念のないIP網にパス(仮想的な通信路)の概念を持ちこむプロトコルである。MPLS網は、IPパケットにコネクションを識別するための新しいフィールド「label」を追加し、ネットワーク上のルータは labelフィールドのlabel値をpop、pushまたはswapしてIPパケットを伝搬する。このMPLSによれば、IPのコネクション型サービスを提供でき、しかも、コネクション毎にセキュリティを確保でき、更に、専用線の代替手段となるIP専用線サービスをIP網で効率良く提供することができ、非常にscalabilityの高い方法である。又、MPLSを使ってVPNを構築する方法がRFC2547BGP/MPLS VPNsとして公開されており、このRFC法により、インターネットワーク上にIP VPNを構成することが出来る。

【００１２】MPLSは、レイヤ2とIP層の中間に位置付けられる。通常のルータはIPパケットのIPヘッダを参照して転送処理を実行するが、MPLS対応ルータはIPヘッダを参照せず、IPヘッダとL2ヘッダ間に設けられるlabel に基づいて転送処理する。図２３はMPLSの説明図であり、1～5はMPLS用ルータであり、MPLSルータ1、5はMPLS網の外部と接続するエッジルータを構成し、MPLSルータ2～4はMPLS網内のコアルータを構成する。エッジルータ1には送信側の端末装置がLAN等を介して接続され、又、エッジルータ5にIPアドレス10.1.100.0/24を有する宛先の端末装置がルータ、LANを介して接続されている。両端末間で通信を行うものとすると、予め、両端末が接続されたエッジルータ1、5間にLDP(label distribution protocol)に従ってLSP(label switched path)がlabelを用いて設定され、このLSPを形成する各MPLSルータ1～4にはラベルテーブル1a～４aが作成される。

【００１３】かかる状態において、送信側端末装置よりIPパケットを含むMACフレームが入力すると、エッジルータ1はテーブルを参照してMACフレームにMPLSのヘッダであるshimヘッダ(後述する)を付加し、該shimヘッダのlabel fieldにlabelとして「39」を付加し(push)、次のMPLSルータ2に向けて送信する。MPLSルータ2はテーブル2aを参照してlabel「39」をlabel「37」に付け替え(swap)、次のMPLSルータ3に向けて送信する。MPLSルータ3もテーブル3aを参照してlabel「37」をlabel「36」に付け替え(swap)、次のMPLSルータ4に向けて送信する。同様に、MPLSルータ4はテーブル4aを参照してlabel「36」に応じたlabel「pop」を求め、labelをヌルにし(pop)、次のMPLSルータ5に向けて送信する。エッジルータ5はlabel=ヌルのフレームを受信すれば、MACフレームよりMPLSのshimヘッダを削除して宛先端末装置に向けて送信する。

【００１４】MPLS用ルータであるLSR(label switching router)は、ルーチングテーブル情報などのIP層の経路情報を参照して経路を決定し、該経路にラベルを張る仕組みを有している。すなわち、LSRはIPのルーチングプロトコル(RIP,OSPFなど)が決めた経路に沿って、LDP(la

bel distribution protocol)に従ってラベルパスを自動的に生成する。

【００１５】図２３はラベルパス設定の仕組みの説明図である。宛先端末装置側のエッジルータであるMPLSルータ(LSR)5はOSPF(open shortest path first)などのルーチングプロトコルを使って送信側MPLSルータ(LSR)1に向かう上流のルータ(LSP)4を求め、該ルータ(LSP)4に対しlabelをヌルにしてフレームを送出するよう依頼すると共に、宛先端末装置のIPアドレス(=10.1.100.0/24)を送る。これにより、MPLSルータ(LSR)4は空いているlabel値(=36)を求め、かつ、ルーチングプロトコルを使って送信側MPLSルータ(LSR)1に向かうMPLSルータLSP3を求め、該MPLSルータLSP4に対しlabelを「36」にしてフレームを送出するよう依頼すると共に、宛先端末装置のIPアドレス(=10.1.100.0/24)を送る。又、MPLSルータLSP4はラベルテーブル4aを作成する。このラベルテーブル4aは、①local label(=36)、② outgoing label(=pop label)、③ prefix (=10.1.100.0/24)、④MPLSルータ(LSR)5とのoutgoing interface(=ether 6)、⑤Next Hop(=MPLSルータ(LSR)5のIPアドレス)を含んでいる。以下、同様に、MPLS用ルータ(LSR)3,MPLS用ルータ(LSR)2はラベルテーブル3a,2aを作成し、又、エッジルータであるMPLSルータ(LSR)1はラベルテーブル1aを作成する。

【００１６】この状態において、宛先IPアドレス10.1.100.0/24のIPパケットを有するMACフレームが送信側端末よりエッジルータ1aに入力すると、図２２で説明したようにMPLS用ヘッダを付加され、label fieldのlabel値をpush, swap, popしながらMPLS網を伝搬し、エッジルータ5aよりMPLS用ヘッダが削除されて宛先端末装置に送信される。

【００１７】図２４はMPLSのヘッダであるシムヘッダ(shim header)の構造とレイヤ2フレーム(MACフレーム)におけるシムヘッダの挿入位置説明図である。図中、M1はMAC宛先アドレス(MAC DA)、M2はMAC発信元アドレス(MAC SA)、M4はタイプ、M5はIPパケット(IPヘッダ/TCPヘッダ/データ部)である。M6はレイヤ2ヘッダとIPヘッダ間に挿入されるシムヘッダであり、20ビットのlabel field、3ビットのEXP field、１ビットのS field、8ビットのTTL fieldを有している。MPLSではシムヘッダのスタック(多重)が可能であり、スタックすることによりVPNを構築することができる。すなわち、図２５（A）に示すように1つのIPパケットに2つのシムヘッダM6,M7を重ねて転送する。図２５（B)に示すように、第1シムヘッダM6のlabel(階層1のlabel)はMPLSネットワーク内部の転送用として使用し、第2のlabel(階層2のlabel)はエッジルータ1,5につながった回線のVPNを識別するため使用する。すなわち、第2のlabelはVPN識別用に使用する。又、ユーザ回線を識別するために第2のlabelを使用することもできる。

【００１８】図２６は２つのlabelをスタックしてIP-VPNを実現するMPLS/VPNの説明図であり、エッジルータ1,5を介してVPN Aのユーザが通信するものとする。予め、エッジルータ1,5はユーザ回線インタフェース単位にVPN-ID(VPN識別子)を割り当てる。図では、エッジルータ1はVPN-Aサイトのネットワークアドレス=192.168.0.Xに対応してVPN-ID=13を割り当て、又、エッジルータ5はVPN-Aサイトのネットワークアドレス=192.168.1.Xに対応してVPN-ID=13を割り当て、VPN-Bサイトのネットワークアドレス=ZZZ.ZZZ.Z.Zに対応してVPN-ID=14を割り当てる。しかる後、受信側エッジルータ5はiBGP(inter border gateway protocol)に従って、VPN-ID/ネットワークアドレスの組み合わせ毎にlabel情報を送信側エッジルータ1に通知する。iBGPはTCPのコネクションを張って経路情報等をやり取りするプロトコルであり、このプロトコルに従ってMPLS網のエッジに位置するルータ同士がコアルータを素通りしてVPN情報の送受をする。図の例では、受信側エッジルータ5はiBGPを使って送信側エッジルータ1に、「192.168.1.X、VPN-ID=13」のラベルは「3」であると通知し、又、「ZZZ.ZZZ.Z.Z、VPN-ID=14のラベルは「4」であると通知する。この情報を基にして、エッジルータ1はVPN-ID毎にラベルテーブル1a, 1bを作成する。

【００１９】以上と並行して、各MPLS用ルータは図２２、図２３で説明したようLDP(labeldistribution protocol)によりパケットをMPLS網内部で転送するためのラベルパスを設定する。これにより、コアルータ2からエッジルータ1に宛先192.168.1.XのMPLS転送用ラベルとして「5」が通知され、又、宛先ZZZ.ZZZ.Z.ZのMPLS転送用ラベルとして「5」が通知され、ラベルテーブル1a, 1bに追加される。以上のラベルテーブル1aが作成された状態において、VPN Aのユーザサイト(送信元VPN-ID=13)からIPパケットが入力すると、エッジルータ1は送信元VPN=13及び宛先IPアドレス=192.168.1.Xに基づいてテーブル1aを参照し、VPN判別用ラベル(=3)、MPLS転送用ラベル(=5)を求め、これら2つのラベルをパケットに付与してコアルータ2に送信する。コアルータ2はMPLS転送用ラベル(=5)を参照して転送処理を行い、受信側エッジルータ5はパケットが到達すると、VPN判別用ラベル(=3)を参照して該当VPNがVPN Aであるとを判断し、ラベルを取り除いてパケットをVPN Aのユーザサイトのみに送出する。尚、以上ではラベルテーブルを２つ設けた例であるが、実際はエッジルータに送信元VPN-IDの数だけテーブルが設けられ、各テーブルに送信元VPN-ID及び宛先IPアドレスの組み合わせに対応させてVPN判別用ラベルとMPLS転送用ラベルとが保持される。

【００２０】図２７はMPLS/VPNsの説明図であり、通信事業者(プロバイダ)のネットワークをMPLS網で構成した例である。11はプロバイダのMPLS網、12,13,14はMPLS網のエッジに位置するプロバイダエッジルータ(PEルータ)、15～18はMPLS網内に位置するコアルータ、21～24

は顧客システム(イントラネット)、25～28はは顧客システムのエッジに位置する顧客エッジルータ(CEルータ)である。PEルータ12～15は2階層のMPLSをサポートし、かつ、VPNを意識するルータである。発信側PEルータはCEルータから入力するパケットに予めテーブルに設定されているVPN判別ラベル(VPN-ID)及びVPN判別用ラベルを付加し、又、受信側のPEルータは該パケットを受信すればそのVPN転送用ラベル(VPN-ID)に応じた顧客システムにパケットを送出する。図２７の例では顧客システム21、22によりVPN Aが形成され、顧客システム23,24によりVPN Bが形成されている。従って、VPN-A内の各顧客システムの端末装置はVPN A内の端末装置にしかアクセスできず、VPN-Bの端末装置にアクセスすることはできない。同様に、VPN-B内の端末装置もVPN-B内の端末装置にしかアクセスできない。以上より、同一企業グループのみに同じVPN-IDを割り当てれば、他の企業グループからアクセスされることはなく、又、他の企業にデータが送信されることはなく、同一企業グループに閉じたIP-VPNを構築することができる。

【００２１】

【発明が解決しようとする課題】VLANによるVPN構築方法によれば、ネットワーク上で各ユーザ毎にユニークなVIDを割り当てることで、容易に、かつ、安い設備投資でVPNを構成できる利点がある。しかし、 VIDフィールドは最大12bitであり、10進数にすると、4,096個までしか設定することができない。この為、4,096個目以降のVIDを要求するユーザが現われた場合に対応できなくなり、小規模から大規模の幅広いネットワークの要請に対応できず、拡張性（スケーラビリティ）が低い問題がある。一方、MPLSによるVPN構築法によれば、VPN識別子を表現するlabel領域は20ビットであるため、VLANによる構築法に比べてはるかに多くのVPNを設定でき、インターネットの拡大に対応でき、拡張性が優れている利点がある。しかし、MPLSによるVPN構築法では、ユーザの近くまで高価なMPLS対応のルータを設置しなくてはならず、しかも、エッジルータの1ポートがユーザのために準備する必要があるなど非常に設備投資がかかる問題がある。

【００２２】以上より、本発明の目的は、ネットワークにおいて、VLAN対応SwitchingHUBでアクセス系ネットワークを構築し、MPLS対応ルータでコアネットワークを構築するようにして安価な値段で且つスケール性の高いVPNを提供することである。又、本発明の別の目的は、VLANとMPLS間にインタフェースを設けることによりVLANとMPLSが共存できるようにし、かつ、VLANからMPLSへの移行を容易に行えるようにして、安価な値段で且つスケール性（拡張性）の高いVPNを提供することである。本発明の別の目的は、地域毎のアクセス系にVLAN対応スイッチングハブを使用し、地域間のWAN上にMPLSによるVPNを構築することで安価な値段で且つスケール性(拡張性)の高いVPNを提供することである。本発明の別の目的は、VPNを構成する際に、IP以外のIPX,FNA,Apple Talk...等のプロトコルもユーザが利用可能な環境を提供することである。

【００２３】

【課題を解決するための手段】上記課題は本発明の第１によれば、共有ネットワーク上にVPNを形成し、該VPNを介して通信を行うネットワークにおいて、ラベルスイッチ網でVPNのコア網を形成すると共に、VLANで該コア網に対するアクセス網を形成し、ラベルスイッチ網とVLAN間のインタフェース機能を実行する装置をこれらラベルスイッチ網の端に設けることにより達成される。このネットワークにおいて、インタフェース装置はMPLS網の端に設けられたエッジルータにより構成でき、送信側のエッジルータはVLANから送出されるパケットをMPLSのパケットに変換してラベルスイッチ網であるMPLS網に送出し、受信側のエッジルータはMPLS網より受信したMPLSのパケットをVLANのパケットに変換し、該VLANパケットを送信側VLANと同一のVPNに属するVLANに向けて送信する。

【００２４】エッジルータは具体的には、VLANのパケットに含まれるVLAN識別子(VID)とMPLSのパケットに含まれるVPN識別子(VPNラベル)の対応を記憶するテーブルを備え、送信側エッジルータはVLANパケットのVIDに応じたVPNラベルを求め、該VPNラベルを有する MPLSパケットを生成してMPLS網に送出し、受信側エッジルータはMPLS網より受信したMPLSパケットに含まれるVPNラベルに応じたVIDを求め、該VIDを有するVLANパケットを生成し、該VIDが示すVLANに送出する。又、エッジルータは、受信側のエッジルータに向けてMPLSパケットを送出する経路を決定するルート決定部、ルート決定部により決定された経路を特定する転送用ラベルを受信側エッジルータのアドレスに対応させて記憶するラベルテーブルを備え、送信側エッジルータは、パケットの宛先MACに応じた受信エッジルータを求め、該ラベルテーブルより受信エッジルータに応じた転送用ラベルを求め、前記VPNラベル及び転送用ラベルを含むMPLSパケットを生成してMPLS網に送出する。

【００２５】又、上記課題は本発明の第２によれば、共有ネットワーク上にVPNを形成し、MPLS網で該VPNのコア網を形成し、VLANで該コア網に対するアクセス網を形成するネットワークにおけるエッジルータにおいて、(1) VLAN識別子(VID)とVPN識別子であるVPNラベルの対応を記憶する手段、(2) 前記対応関係を用いてVLANから送出されるパケットに含まれるVIDに応じたVPNラベルを求め、該VPNラベルを含むMPLSパケットを生成してMPLS網に送出するMPLSパケット生成部を備えた送信側エッジルータにより達成される。このエッジルータは更に、(3) 受信側のエッジルータに向けてMPLSパケットを送出する経路を決定するルート決定部、(4) ルート決定部により

決定された経路を特定する転送用ラベルを受信側エッジルータに対応させて記憶する転送用ラベル記憶部を備え、(5) 前記MPLSパケット生成部は、パケットの宛先MACアドレスに応じた受信エッジルータを求め、ラベル記憶部より該受信エッジルータに応じた転送用ラベルを求め、前記VPNラベル及び転送用ラベルを含むMPLSパケットを生成する。

【００２６】又、上記課題は本発明の第３によれば、共有ネットワーク上にVPNを形成し、MPLS網で該VPNのコア網を形成し、VLANで該コア網に対するアクセス網を形成するネットワークにおけるエッジルータにおいて、(1) VLAN識別子(VID)とVPN識別子であるVPNラベルの対応を記憶するテーブル、(2) 前記テーブルを用いてMPLS網より入力するパケットに含まれるVPNラベルに応じたVIDを求め、該VIDを含むVLANパケットを生成してMPLS網に送出するVLANパケット生成部、を備えた受信側のエッジルータにより達成される。

【００２７】又、上記課題は本発明の第４によれば、共有ネットワーク上にVPNを形成し、MPLS網で該VPNのコア網を形成し、VLANで該コア網に対するアクセス網を形成するネットワークにおけるエッジルータにおいて、(1) VLAN識別子(VID)とVPN識別子であるVPNラベルの対応を記憶するテーブル、(2) 前記テーブルを用いてVLANより入力するパケットに含まれるVIDに応じたVPNラベルを求め、該VPNラベルを含むMPLSパケットを生成してMPLS網に送出するMPLSパケット生成部、(3) 前記テーブルを用いてMPLS網より入力するパケットに含まれるVPNラベルに応じたVIDを求め、該VIDを含むVLANパケットを生成してMPLS網に送出するVLANパケット生成部、を備えたエッジルータにより達成される。

【００２８】

【発明の実施の形態】（Ａ）本発明の概略

図１は本発明のVLANとMPLS混在ネットワークの概略図であり、101～104は拠点Ａ～ＤのVLANであり所定のVID(VLAN ID)で管理されている。110はインターネット(WAN)上にMPLSにより構築されたlabelで管理される共有ネットワーク(MPLSネットワーク)、111～114はMPLS網のエッジ部に設けられたエッジルータである。送信側のエッジルータ111～114はVLAN101～104から入力するVLANパケット(図２０）をMPLSパケット（図２５(A)）に変換して送信し、受信側のエッジルータはMPLSパケットをVLANパケットに変換して所定のVLANに出力する。

【００２９】すなわち、送信側エッジルータは、VLANパケットに含まれるVIDをVPN識別子であるVPNラベルに変換すると共に、VLANパケットの宛先に基づいて該パケットを所定の経路に沿って転送するための転送用ラベルを求め、VIDに替えてこれらラベルを付加してMPLSパケットを生成してMPLS網110に送出する。MPLS網110は予め設定されているルートにそって転送用ラベルを付け替えながらMPLSパケットを目的の受信側エッジルータまでルーチングする。受信側エッジルータはMPLS網よりMPLSパケットを受信すれば、転送用ラベルを削除すると共に、VPNラベルを元のVIDに変換し、ラベルに替えて該VIDを付加してVLANパケットを生成し、該VLANパケットをVIDが示すVLANに送出する。以上、所定のVPNに属する送信側VLANから同一のVPNに属する受信側VLAにパケットを送信することができる。

【００３０】図２はエッジルータ111の概略構成図であり、他のエッジルータも同一の構成を備えている。エッジルータ111のラインカード部121はEthernetインタフェースの機能を備え、所定のVLANよりVLANパケットを受信する。VPN識別部122は受信したVLANパケットのVIDを参照してVPNを識別し、該VPNに応じたタグ/ラベル変換部(サブルータ)123i(i=1,2,...)へ入力する。識別されたVPNに応じたサブルータ123iのテーブル124には例えば図４に示すように、①VLAN ID(VID)と、②該VIDにより特定されるVLANが所属するVPNを特定するVPN識別子（VPNラベル）の対応が予め記憶されている。又、ルート決定部131は、ルーチングプロトコル132を用いて受信側エッジルータへの経路を予め決定し、MPLS網ルーチングテーブル(転送用ラベル記憶部)133に受信側エッジルータのIPアドレスに対応させて前記決定した経路を特定する転送用ラベル(pushラベル)を記憶する。

【００３１】サブルータ123iは、パケットが入力すると、タグに含まれるVIDに応じたVPN識別子(VPNラベル)をテーブル124より求める。又、サブルータ123iはパケットに含まれる宛先アドレスに基づいて受信側エッジルータを求め、該エッジルータのIPアドレスに対応させて記憶されている転送用ラベルをMPLS網ルーチングテーブル133より求める。ラベルが求まれば、サブルータ123iはパケットのタグに替えてVPNラベル及び転送用ラベルを挿入し(swap)、ラインカード部128を介してMPLS網111に送出する。以後、MPLS網110は予め設定されている経路にそって転送用ラベルを付け替えながらMPLSパケットを目的の受信側エッジルータまでルーチングする。受信側エッジルータのラインカード部128はMPLS網110よりMPLSパケットを受信し、VPN識別部129はMPLSのVPNラベルを参照してVPNを識別し、該VPNに応じたサブルータ123i(i=1,2,...)へ入力する。

【００３２】サブルータ123iは転送用ラベルを削除する共に、テーブル124を参照してVPNラベルに応じたVIDを求める。ついで、VPNラベルに替えて求めたVIDを含むタグを付加してVLANパケットを生成し、該VLANパケットをVLAN側のラインカード部　121を介してVIDが示すVLANに送出する。尚、各エッジルータ111～114におけるテーブル124の内容は同一でなく、同一のVPNに属するVLANのVID値は同じとは限らない。また、図２では明確に示さなかったが、サブルータは図５に示すように　VPN毎に存在する。以上より、図１において拠点AのVLAN 101から拠点DのVLAN 104に通信が発生すると、図３に示すよう

にタグとラベルのスワップがエッジルータ111,１１４で行なわれる。これにより送信側VLANより入力するVLANパケットはエッジルータ111でMPLSパケットとなってMPLS網を伝送し、エッジルータ114でVLANパケットに変換され、送信側VLANと同一のVPNに属するVLANに送信される。

【００３３】（Ｂ）MPLSによる企業のネットワーク形態
図６はMPLS網を用いた企業のネットワーク形態説明図であり、200は共有ネットワークであるインターネット上に形成されたMPLS網、201はVLAN Domain 東京、202はVLAN Domain 名古屋、203はVLAN Domain大阪、204はインターネット、205はファイアウォール(FW)であり、各VLAN Domain には複数の企業のVLANが構成されている。MPLS網200と各VLAN Domain201～203間であって、MPLS網のエッジにはVLANを終端するプロバイダエッジルータ(Provider Edge Router:PE)211～213が設けられている。

【００３４】VLAN Domain 東京201には東京地区のＡ企業のVLAN(VID=101)、Ｂ企業のVLAN(VID=2)が形成されている。Ａ企業のVLAN(VID=101)を構成するCPEルータ(CustomerPreequipment Edge Router)212は、EthernetによりL2Switch(スイッチングハブ)213を介してエッジルータPE 211の第1のポートに接続している。又、Ｂ企業のVLAN(VID=2)を構成するCPEルータ214は、Ethernetを介してL2Switch(スイッチングハブ)215に接続され、該スイッチングハブ215はエッジルータPE 211の第2のポートに接続されている。VLAN Domain 名古屋202には名古屋地区のＡ企業のVLAN(VID=152)、Ｃ企業のイントラネットが形成されている。Ａ企業のVLAN(VID=152)を構成するCPEルータ221は、EthernetによりL2Switch(スイッチングハブ)222を介してエッジルータPE212の第1のポートに接続している。又、Ｃ企業のイントラネット223のCPEルータ224は、エッジルータPE 212の第2のポートに接続されている。VLAN Domain 大阪203には大阪地区のＡ企業のVLAN(VID=1501)、Ｃ企業のイントラネットが形成されている。Ａ企業のVLAN(VID=1501)を構成するCPEルータ231は、EthernetによりL2Switch(スイッチングハブ)232を介してエッジルータPE 213の第1のポートに接続している。又、Ｃ企業のイントラネット233のCPEルータ234は、エッジルータPE 213の第2のポートに接続されている。

【００３５】各地区におけるＡ企業のVLAN(VID=101), VLAN(VID=152), VLAN(VID=1501)は同一のVPNを構成している。従って、Ａ企業側からMPLS網側を見ると、図７（Ａ）に示すように各CPEルータ212, 221, 231 がレイヤ2のスイッチングハブSHBに接続されているように見え、Ａ企業のネットワークはコア網をMPLS網で構成し、アクセス網をVLANで構成してなるL2(VLAN) over MPLSネットワーク形態となる。又、Ｂ企業からMPLS網側を見ると、図７（Ｂ）に示すようにCPEルータ214及びファイアウォール205がレイヤ2/3のスイッチングハブSHB´に接続されているように見え、Ｂ企業のネットワークはインターネット接続形態となる。又、Ｃ企業からMPLS網側を見ると、図７（Ｃ）に示すようにイントラネット223, 233のCPEルータ224、234がルータRTに接続されているように見え、Ｃ企業のネットワークはMPLSでVPNを構成したMPLS/VPNsネットワーク形態となる。

【００３６】（Ｃ）L2(VLAN) over MPLSネットワーク
図８は図６よりＡ企業に関連する部分を書き出した本発明のL2(VLAN) overMPLSネットワークの全体図であり、図６と同一部分には同一符号を付し、VLANを構成するルータCPEA 212, 221, 231にはL2アドレスであるMACアドレスMAC A, MAC B, MAC Cが付されている。

【００３７】（Ｄ）エッジルータの構成
各エッジルータPEA～PECは同一の構成を備えている。図９はエッジルータの構成図であり、図２に示したエッジルータを詳細に示すもので、図２のエッジルータと同一部分には同一符号を付している。ラインカード部121はEthernetインタフェースの機能を備え、所定のVLANよりVLANパケットを受信する。VPN識別部122は受信したVLANパケットのVIDを参照してVPNを識別し、VPNに応じたサブルータ123i(i=1,2,...)へパケットを入力する。サブルータ123iのVPNラベルテーブル124には図１０に示すように、①VPNラベル(VPN識別子)、②配下であるCPEルータのL2アドレス(MACアドレス)、③出力側インタフェース、④エッジルータに接続するVLANの識別子(VID)、⑤VPNi (VPNinstance :VPN識別子の便宜名)の対応が予め記憶されている。

【００３８】又、L2VPNルーチングテーブル125には、図１０に示すようにVPNを構成するVLAN毎に、①該VLAN内のCPEルータのL2アドレス(MAC アドレス)、②CPEルータが接続するエッジルータのループバックアドレス(IPアドレス)、③CPEルータの属するVLANの識別子(VID)を保持する。図８の例では、VLAN(VID=101),VLAN(VID=152),VLAN(VID=1501)のそれぞれに対応させて、①CPEルータ212,221,231のMAC アドレスMAC A, MAC B, MAC C、②各CPEルータが接続するエッジルータ(PEA, PEB, PEC) 211, 212, 213のループバックアドレス(IPアドレス)、③各CPEルータの属するVLANのVID(=101,152,1501)が保持されている。

【００３９】MPLS網ルーチングテーブル(転送用ラベルテーブル)133は受信エッジルータへの経路を特定する通信用ラベルを記憶する。同一VPNに属するVLAN間で通信できるように、予めMPLS網内のルータのルート決定部はルーチングプロトコルを用いて送信側エッジルータから受信側エッジルータに至る経路を探索し、LDP (Label Distribution Protocol)に従って各経路にLabelを割り当てる。従って、送信側エッジルータのルート決定部131は、ルーチングプロトコル132を用いて受信側エッジルータへの経路を決定し、転送用ラベルテーブル133に受信側エッジルータのループバック(IPアドレス)に対応さ

せて前記決定した経路を特定する転送用ラベル(pushラベル)を記憶する。

【００４０】サブルータ123iのVPNラベル処理部126は、VLANパケット（図２0参照）が入力すると、タグに含まれるVIDに応じたVPN識別子(VPNラベル)をVPNラベルテーブル124より求める。又、ルーチングテーブル処理部127はVLANパケットに含まれる宛先MACアドレスに基づいてL2 VPNルーチングテーブル125より出力側エッジルータのループバックアドレスを求め、ついで、転送用ラベルテーブル133より該ループバックアドレス(IPアドレス)に対応する転送用ラベル(pushラベル)を求める。VPNラベル、pushラベルが求まれば、サブルータ123iは図３に示すようにタグに替えてVPNラベル及び転送用ラベルを挿入してMPLSパケットを生成し(swap)、該MPLSパケットをラインカード部128を介してMPLS網に送出する。

【００４１】以後、予め設定されているMPLS網内の経路にそって転送用ラベルを付け替えながらMPLSパケットが目的の受信側エッジルータに到達する。受信側エッジルータのラインカード部128はMPLS網110よりMPLSパケットを受信し、VPN識別部129はMPLSのVPNラベルを参照してVPNを識別し、該VPNに応じたサブルータ123i(i=1,2,...)へ入力する。サブルータ123iは転送用ラベルを削除する共に、VPNラベルテーブル124を参照してVPNラベルに応じたVIDを求める。ついで、VPNラベルに替えて求めたVIDを含むタグを付加してVLANパケットを生成し(swap)、該VLANパケットをラインカード部121を介してVIDが示すVLANに送出する。尚、各エッジルータ211～213(図８)におけるVPNラベルテーブル124の内容は同一でなく、同一のVPNに属するVLANのVID値は同じとは限らない。また、図９では明確に示さなかったが、サブルータ123i(i=1,2,..)や転送用ラベルテーブル133はVPN毎に存在する。

【００４２】（Ｅ）VPNテーブルの生成

VPNに属するVLAN同士で通信を行えるようにするには、(1) 予めこれらVLANが接続するエッジルータ間のルートを設定し、該ルートに沿ったルータの転送用ラベルテーブル133(図９）に転送用ラベルを記憶し、かつ、(2) VPNラベルテーブル124、L2VPNルーチングテーブル125を作成する必要がある。(1)の転送用ラベルテーブル133の作成方法は周知であるため説明はしない。VPNラベルテーブル124、L2VPNルーチングテーブル125を作成するには、図１０（Ａ）に示すように、まず、VPNの識別子(VPNラベル)、VLAN識別子(VID)、VPNiをオペレータが手入力する。これらデータがエッジルータに入力されると、該エッジルータのVPNラベル処理部126は、自分に接続するVLANのCPEルータのMACアドレスをARP(Address Resolution Protocol)を使って求め、又、pushラベルが付されたMPLSパケットを送出する経路のインタフェースを求め、図１０（Ｂ）に示すように設定してVPNラベルテーブル124を作成する。

【００４３】ついで、ルーチングテーブル処理部127は、自エッジルータに接続するCPEルータのMACアドレス及びVLAN識別子(VID)をVPNラベルテーブル124より求めてL2VPNルーチングテーブル125のdirectConnect情報を作成する(図１０（Ｂ）参照）。しかる後、VPNを構成する各VLAN(VID=101,152,1501)と接続するエッジルータ(PEA, PEB, PEC)211, 212, 213はそれぞれiBGPを用いて、自エッジルータに接続するユーザルータCPEのMACアドレスと自エッジルータのループバックアドレス（IPアドレス）,VIDを組にして他のエッジルータに送出する。これにより、各エッジルータは受信情報に基づいてL2VPNルーチングテーブル125を完成する(図１０（Ｂ）参照）。以上により、各エッジルータ211, 212, 213のそれぞれには図８のＡ企業のVPNについて図１１（Ａ）～（Ｃ）に示すVPNテーブルが作成される。

【００４４】（Ｆ）CPEAからCPECへの通信例

図１２は東京のＡ企業のVLAN(VID=101)に属するユーザルータCPEAから大阪のＡ企業のVLAN(VID=1501)に属するユーザルータCPECにパケットを送信する送信例である。ユーザルータCPEAはVID=101を有するタグが付加されたVLANパケットPKT1を送出する。エッジルータPEA 211はパケットPKT1が入力するとタグを外し、代わりにVPNラベル(=26:企業ＡのVPN識別子）と転送用ラベル(=pushラベル)を付加してなるMPLSパケットPKT2を生成してMPLS網200に送出する。以後、MPLSパケットPKT2は予め設定されているMPLS網内の経路にそって転送用ラベルを付け替えながら目的の受信側エッジルータPEC 213に到達する。受信側エッジルータPEC 213はラベルを外し、宛先のユーザルータCPECが属するVLAN識別子(VID=1501)を付加してVLANパケットPKT3を作成し、VID=1501が指示するVLANに送出する。これにより、VLANパケットPKT3はユーザルータ231に到達する。

【００４５】（Ｇ）L2(VLAN) over MPLSの送信処理

図１３及び図１４はL2(VLAN) over MPLSの送信処理フローである。送信側エッジルータはパケットが入力すると該パケットにタグが付加されているかチェックし(ステップ301)、付加されていなければMPLSパケットであるから通常のMPLSの処理を行い、タグが付加されていれば、該タグに含まれるVLAN ID(=VID)の値を抽出し(ステップ302)、VID値が4096以上であるかチェックする(ステップ303)。4096以上であれば、VID値の範囲0～4095を越えているため該パケットを破棄する。しかし、VID値が0～4095の範囲に入っていれば、VLAN IDとVPNラベルの変換テーブル124を参照し(ステップ 304)、VPNラベル値が発見されたかチェックする(ステップ305)。発見されなければ通常のMPLS対応の処理を行い、発見されれば、タグを外して2層目のラベル値(VPNラベル)をつける（ステップ306)。

【００４６】しかる後、パケットの宛先MACアドレスより受信側エッジルータのループバックアドレス(IPアド

レス)をL2VPNルーチングテーブル125より求める(ステップ307)。ループバックアドレスが求まれば、転送用ラベルテーブル133を参照して転送用ラベル(pushラベル)を求め(ステップ308)、該pushラベルを1階層目につけてMPLS網に送出する(ステップ309)。以上は送信側エッジルータの処理である。以後、MPLS網内でのラベルルーチング処理が行われ、MPLSパケットは予め設定されているMPLS網内の経路にそって転送用ラベルを付け替えながら目的の受信側エッジルータに向けて転送される(ステップ310)。

【００４７】受信側エッジルータはMPLSパケットが到着したかチェックし(ステップ311)、到着すれば、１階層目に付属されている転送用ラベルを削除する（ステップ312)。ついで、２階層目のVPNラベルを抽出し(ステップ313)、VLAN ID(=VID)とVPNラベルとの対応テーブル124を参照し(ステップ314)、VIDが発見されたかチェックする(ステップ315)。VIDが発見されなければパケットを破棄し、VIDが発見されれば、2階層目のラベルを外し、該VIDを含むタグをつけてVLANパケットを作成する(ステップ316)。ついで、VPNラベルテーブル124を参照して出力インタフェースを求め、該インタフェースにVLANパケットを送出し(ステップ317)、宛先のユーザルータCPECはVLANパケットを受信して所定の処理を行う(ステップ318)。

【００４８】（Ｈ）VPNテーブルの更新処理

VPNの構成は企業ポリシーにより拡大、変更が行われて刻々と変化する。そこで、VPNの構成変化に応じてVPNテーブル124、125を更新する必要がある。図１５はユーザルータCPEAがユーザルータCPECと通信する場合の更新説明図である。

1．ユーザルータCPEA 212は宛先のユーザルータCPECのMACアドレスが不明であれば、ルータCPECの IPアドレスを含むARPパケットをブロードキャストする。

2．エッジルータPEA 211は該ARPパケット(ブロードキャストパケット)を受信すれば、該パケットのコピーを作成し、他のエッジルータPEB，PEC 212,213に流す。

3．ユーザルータCPECは自分のIPアドレスを含むARPパケットを受信すれば、ARP-replyパケットに自分のMACアドレスを乗せて返送する。各エッジルータPEはARP-replyパケットによりVPNラベルテーブル124,VPNルーチング125における各CPEのMACアドレスを自動的に更新する。

4．又、定期的に、各ルータの IPアドレスを含むARPパケットをブロードキャストして各テーブルを更新する。

【００４９】（Ｉ）同一VPNに属するVLAN同士の通信を禁止する処理

図１０、図１１を参照して説明したVPNテーブルの作成処理では、VLAN同士が自由に通信を行える場合であったが、同じVPNに属していても所定VLAN同士の通信を禁止したい場合がある。かかる場合、通信禁止のVLANが属するエッジルータ間においてiBGPによるルーチング情報の通信を停止する。このようにすれば、L2VPNルーチングテーブル125に通信禁止先ルータCPEの MACアドレス、該ルータCPEが接続するエッジルータのループバックアドレス(IPアドレス)が登録されなくなり、通信を行うことができなくなる。

【００５０】図１６は通信禁止のVLANが存在する場合のL2VPNルーチングテーブル125の作成処理フローである。所定VPNについて、各エッジルータPEにVLAN ID(VID)及びVPN識別子(VPNラベル)を設定入力する(ステップ401)。ついで、通信禁止VLANのペアを入力する(ステップ402)。各エッジルータPEはVPNラベルテーブルを自動作成し(ステップ403)、ついで、各エッジルータPEはL2VPNルーチングテーブル125のdirectConnect 情報を作成する(ステップ404)。

【００５１】しかる後、iBGPを使って、VPNルーチング情報(ユーザルータCPEの MACアドレス、エッジルータのループバックアドレス等)を通信禁止されていないVLANが配下となっているエッジルータPEに送信する(ステップ405)。しかし、通信禁止されているVLANが配下となっているエッジルータPEにはVPNルーチング情報を送信しない。各エッジルータPEは他のエッジルータから送られてくるルーチング情報を受信し、該ルーチング情報を用いてL2VPNルーチングテーブル125を作成する(406)。以上により、エッジルータPEのL2VPNルーチングテーブル125には通信禁止先ルータCPEの MACアドレス、該ルータCPEが接続するエッジルータアドレスが登録されない。この結果、転送用ラベルを取得することができず通信禁止先のVLAとは通信を行うことができなくなる。

【００５２】（Ｊ）VLANのuser priority とMPLSにおけるIP Precedence

図１７（Ａ）に示すようにVLANパケットのタグは3ビットのuser priorityを含み、この3ビットで各MACで規定されたプライオリティを入れるようになっている。プライオリティ値は0～7の8レベルがあり、数値が小さければ(例えば0)、ユーザプライオリティが低くく、数値が大きければプライオリティが高い。一方、図１８（Ｂ）に示すようにMPLSパケットのラベルは3ビットの実験用フィールドEXPを含み、この3ビットを用いてIP Precidenceを表現する。このIP Precidenceもプライオリティ値は0～7の8レベルがあり、数値が小さければ(例えば0)、プライオリティが低くく、数値が大きければプライオリティが高い。そこで、エッジルータでVLANパケットからMPLSパケットに変換する際、3ビットのuser priorityをEXPフィールドに挿入し、又、MPLSパケットから VLANパケットに変換する際、3ビットのEXP フィールドのIP Precidennceをuser priority フィールドに挿入する。このようにすれば、VLANにおける優先制御をMPLS網におけるIPPrecidence制御として継続でき、又、IP Precidence制御から元のVLANにおける優先制御に戻すことができる。

【００５３】・付記
（付記１）共有ネットワーク上にVPNを形成し、該VPNを介して通信を行うネットワークにおいて、ラベルスイッチ網でVPNのコア網を形成すると共に、VLANで該コア網に対するアクセス網を形成し、ラベルスイッチ網とVLAN間のインタフェース機能を実行する装置をこれらラベルスイッチ網の端に設けた、ことを特徴とするネットワーク。
【００５４】（付記２）前記インタフェース装置は、ラベルスイッチ網であるMPLS網の端に設けられたエッジルータであり、送信側のエッジルータはVLANから送出されるパケットをMPLSのパケットに変換してMPLS網に送出し、受信側のエッジルータはMPLS網より受信したMPLSのパケットをVLANのパケットに変換し、該VLANパケットを送信側VLANと同一のVPNに属する VLANに向けて送信する、ことを特徴とする付記１記載のネットワーク。
【００５５】（付記３）前記エッジルータはVLANのパケットに含まれるVLAN識別子(VID)とMPLSのパケットに含まれるVPNラベルの対応を記憶するテーブルを備え、送信側エッジルータはVLANパケットのVIDに応じたVPNラベルを求め、該VPNラベルを有するMPLSパケットを生成してMPLS網に送出し、受信側エッジルータはMPLS網より受信したMPLSパケットに含まれるVPNラベルに応じたVIDを求め、該VIDを有するVLANパケットを生成し、該VIDが示すVLANに送出する、ことを特徴とする付記２記載のネットワーク。
【００５６】（付記４）前記エッジルータは、受信側のエッジルータに向けてMPLSパケットを送出する経路を決定するルート決定部、ルート決定部により決定された経路を特定する転送用ラベルを受信側エッジルータのアドレスに対応させて記憶するテーブルを備え、送信側エッジルータは、パケットの宛先MACアドレスに応じた受信エッジルータを求め、該テーブルより受信エッジルータに応じた転送用ラベルを求め、前記VPNラベル及び転送用ラベルを含むMPLSパケットを生成してMPLS網に送出する、ことを特徴とする付記３記載のネットワーク。
【００５７】（付記５）前記VPNを構成するVLANに接続するエッジルータはそれぞれ、該エッジルータに接続するVLAN構成装置のアドレスとエッジルータのアドレスを組にして前記他のエッジルータに送出し、各エッジルータは受信情報に基づいてレイヤ2ルーチングテーブルを作成し、送信側エッジルータは、該レイヤ2ルーチングテーブルより前記パケットの宛先に応じた受信エッジルータを求める、ことを特徴とする付記４記載のネットワーク。
【００５８】（付記６）エッジルータは通信が禁止されているVLANが接続されたエッジルータに上記のアドレス情報を送信しない、ことを特徴とする付記５記載のネットワーク。
（付記７）送信側エッジルータは、VID値が設定値以上のVLANパケットを廃棄することを特徴とする付記２記載のネットワーク。
（付記８）送信側エッジルータはVLANパケットのタグに含まれるユーザ優先情報をMPLS網のIP優先情報としてMPLSパケットのラベルに挿入し、受信側エッジルータはMPLSパケットのラベルに含まれるIP優先情報をVLANのユーザ優先情報としてVLANパケットのタグに挿入する、ことを特徴とする付記２記載のネットワーク。
【００５９】（付記９）共有ネットワーク上にVPNを形成し、MPLS網で該VPNのコア網を形成し、VLANで該コア網に対するアクセス網を形成するネットワークにおけるエッジルータにおいて、VLAN識別子(VID)とVPN識別子であるVPNラベルの対応を記憶する手段、前記対応関係を用いてVLANから送出されるパケットに含まれるVIDに応じたVPNラベルを求め、該VPNラベルを含むMPLSパケットを生成してMPLS網に送出するMPLSパケット生成部、を備えたことを特徴とする送信側エッジルータ。
【００６０】（付記１０）前記エッジルータは更に、受信側のエッジルータに向けてMPLSパケットを送出する経路を決定するルート決定部、ルート決定部により決定された経路を特定する転送用ラベルを受信側エッジルータに対応させて記憶する転送用ラベル記憶部、を備え、前記MPLSパケット生成部は、パケットの宛先MACアドレスに応じた受信エッジルータを求め、該転送用ラベル記憶部より受信エッジルータに応じた転送用ラベルを求め、前記VPNラベル及び転送用ラベルを含むMPLSパケットを生成する、ことを特徴とする付記９記載のエッジルータ。
【００６１】（付記１１）前記MPLSパケット生成部は、前記VPNを構成する他のVLANに接続するエッジルータより送られてくる該エッジルータのアドレスと該エッジルータに接続するVLAN構成装置のアドレスとの組み合わせ情報に基づいてレイヤ2ルーチングテーブルを作成し、該レイヤ2ルーチングテーブルよりパケットの宛先に応じた前記受信エッジルータを求める、ことを特徴とする付記１０記載のエッジルータ。
【００６２】（付記１２）共有ネットワーク上にVPNを形成し、MPLS網で該VPNのコア網を形成し、VLANで該コア網に対するアクセス網を形成するネットワークにおけるエッジルータにおいて、VLAN識別子(VID)とVPN識別子であるVPNラベルの対応を記憶するテーブル、前記テーブルを用いてMPLS網より入力するパケットに含まれるVPNラベルに応じたVIDを求め、該VIDを含むVLANパケットを生成してMPLS網に送出するVLANパケット生成部、を備えたことを特徴とする受信側のエッジルータ。
【００６３】（付記１３）共有ネットワーク上にVPNを形成し、MPLS網で該VPNのコア網を形成し、VLANで該コア網に対するアクセス網を形成するネットワークにおけるエッジルータにおいて、VLAN識別子(VID)とVPN識別子であるVPNラベルの対応を記憶するテーブル、前記テー

ブルを用いてVLANより入力するパケットに含まれるVIDに応じたVPNラベルを求め、該VPNラベルを含むMPLSパケットを生成してMPLS網に送出するMPLSパケット生成部、前記テーブルを用いてMPLS網より入力するパケットに含まれるVPNラベルに応じたVIDを求め、該VIDを含むVLANパケットを生成してMPLS網に送出するVLANパケット生成部、を備えたことを特徴とするエッジルータ。

【００６４】（付記１４）エッジルータは更に、受信側のエッジルータに向けてMPLSパケットを送出する経路を決定するルート決定部、ルート決定部により決定された経路を特定する転送用ラベルを受信側エッジルータに対応させて記憶する転送用ラベル記憶部、を備え、前記MPLSパケット生成部は、パケットの宛先に応じた受信エッジルータを求め、該転送用ラベル記憶部より受信エッジルータに応じた転送用ラベルを求め、前記VPNラベル及び転送用ラベルを含むMPLSパケットを生成する、ことを特徴とする付記１３記載のエッジルータ。

【００６５】（付記１５）前記MPLSパケット生成部は、前記VPNを構成する他のVLANに接続するエッジルータより送られてくる該エッジルータのアドレスと該エッジルータに接続するVLAN構成装置のアドレスとの組み合わせ情報に基づいてルーチングテーブルを作成し、該ルーチングテーブルよりパケットの宛先に応じた前記受信エッジルータを求める、ことを特徴とする付記１４記載のネットワーク。

【００６６】

【発明の効果】以上本発明によれば、MPLSのVPN識別子(VPNラベル)を20ビットで表現でき、キャリアネットワークのコア部分においてこのMPLSを使用することにより、VLANによる構築法に比べてはるかに多くのVPNを設定でき、VLANによるVPN数の限界値4,096の問題をクリアでき、スケール性の高いVPNを提供できる。又、本発明によれば、VLAN対応SwitchingHUBでアクセス系ネットワークを構築し、MPLS対応ルータでコアネットワークを構築することにより、安価なVPN(L2(VLAN) over MPLS形態のネットワーク)を構築できる。すなわち、本発明によれば、高価なMPLS対応ルータを地域内に設置せず、地域毎のアクセス系にVLAN対応スイッチングハブを使用し、かつ、地域間のWAN上にMPLSによるVPNを構築することで安価な値段で且つスケール性(拡張性)の高いVPNを提供することができる。

【００６７】又、本発明によれば、VLANとMPLS間にパケット変換を行うインタフェース(エッジルータ)を設けたから、VLANとMPLSのネットワークを共存させたり、VLANからMPLSの移行を容易に行うことができ、安価な値段で且つスケール性の高いVPNを提供することができる。

又、本発明によれば、VLANとMPLSの統合するネットワーク手法、技術、製品を提供できるようにしたから、VLANで組まれた既存ネットワークを容易にL2(VLAN)over MPLSに移行することが出来る。

【図面の簡単な説明】

【図１】本発明のVLANとMPLSの混在ネットワークの概略図である。

【図２】エッジルータの概略構成図である。

【図３】VLANとMPLSのパケットの交換説明図である。

【図４】VIDとVPNラベルの変換テーブルである。

【図５】エッジルータの別の構成図である。

【図６】MPLS利用による企業のネットワーク形態説明図である。

【図７】企業のネットワーク形態説明図である。

【図８】L2 over MPLSネットワークである。

【図９】PEルータ(エッジルータ)の内部構造である。

【図１０】VPNテーブルの生成説明図である。

【図１１】各エッジルータにおける企業のVPNテーブル説明図である。

【図１２】CPEAからCPECへの送信説明図である。

【図１３】L2(VLAN) over MPLSの送信処理フロー(その1)である。

【図１４】L2(VLAN) over MPLSの送信処理フロー(その2)である。

【図１５】CPEAからCPECへ通信する場合における学習説明図である。

【図１６】通信禁止VLANが存在する場合におけるL2VPNテーブル作成処理フローである。

【図１７】VLANにおけるユーザプライオリティとMPLSにおけるIP Precedenceの対応説明図である。

【図１８】ポートベースVLANの構成例である。

【図１９】複数のスイッチングハブに属するポートをグループ化したVLAN構成例である。

【図２０】VLANのMACフレームフォーマットである。

【図２１】VLANの実現例である。

【図２２】MPLS説明図である。

【図２３】ラベル設定の仕組み説明図である。

【図２４】シムヘッダの構造及び挿入位置説明図である。

【図２５】シムヘッダのスタック説明図である。

【図２６】MPLS/VPNの説明図である。

【図２７】MPLS/VPNsの説明図である。

【符号の説明】

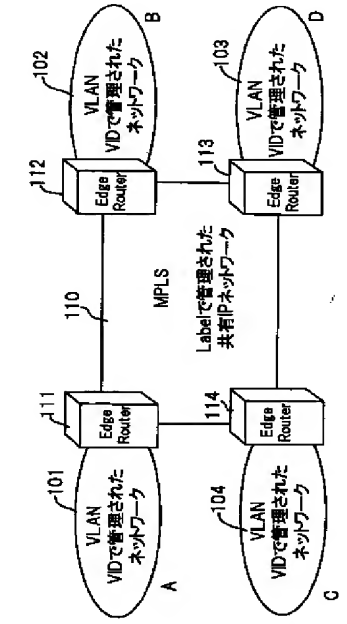
101～104・・拠点Ａ～ＤのVLAN

110・・MPLSネットワーク

111～114・・MPLS網のエッジ部に設けられたエッジルータ

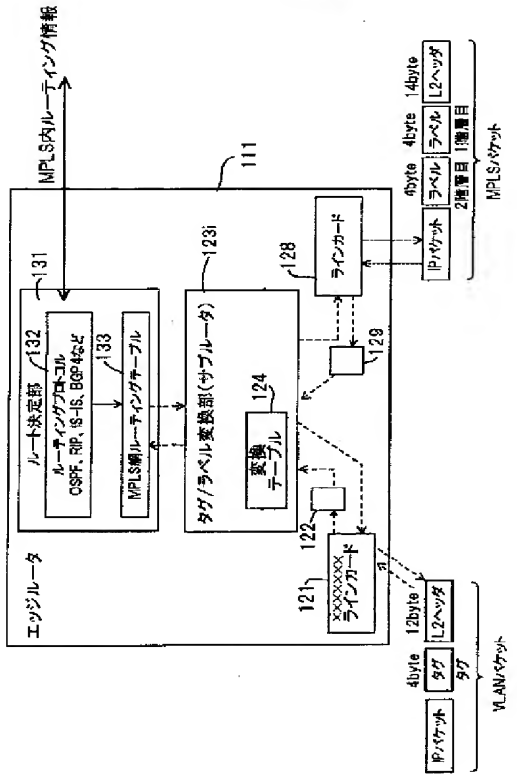
【図１】

本発明のVLANとMPLSの混在ネットワークの概略図



【図２】

エッジルータの概略構成



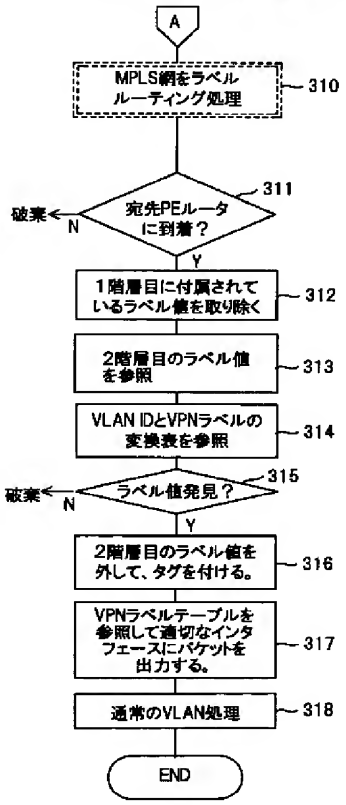
【図４】

VIDとLabelの変換テーブル

VLAN ID(VID)	VPN ラベル
N	M
N+1	M+1
.	.
.	.
.	.
N'	M'

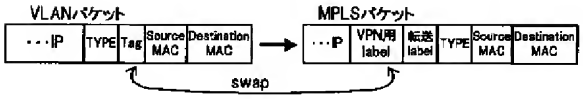
【図１４】

L2(VLAN) over MPLSの送信処理(その2)



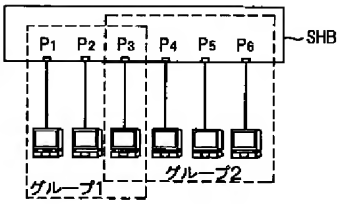
【図３】

VLANとMPLSのパケットの交換説明図

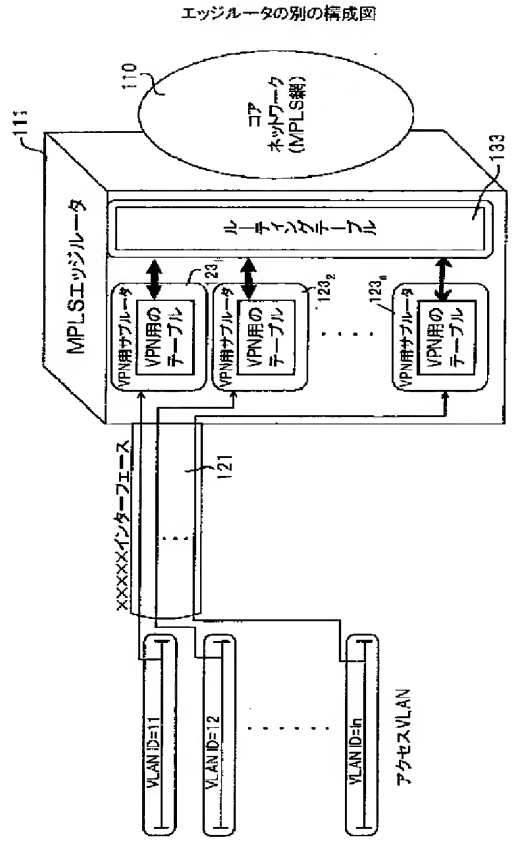


【図１８】

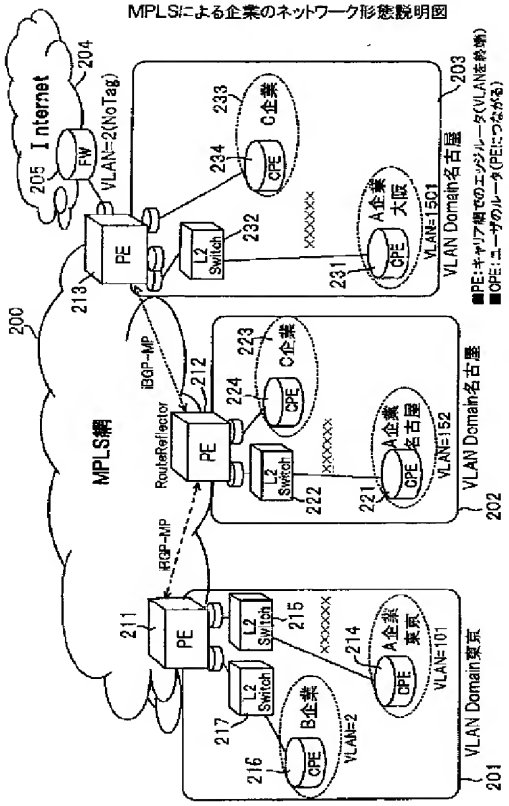
ポートベース VLANの構成例



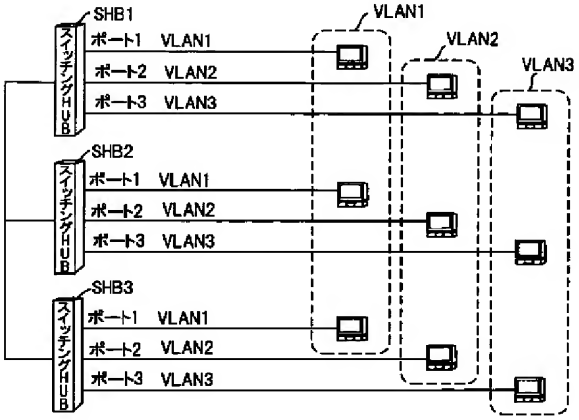
【図5】


エッジルータの別の構成図
110
コア
ネットワーク
(MPLS網)
111
MPLSエッジルータ
133
ルーティングテーブル
VPN用サブルータ
VPN用の
テーブル
23
123₂
123n
121
XXXXXインターフェース
VLAN ID=11
VLAN ID=12
VLAN ID=n
アクセスVLAN

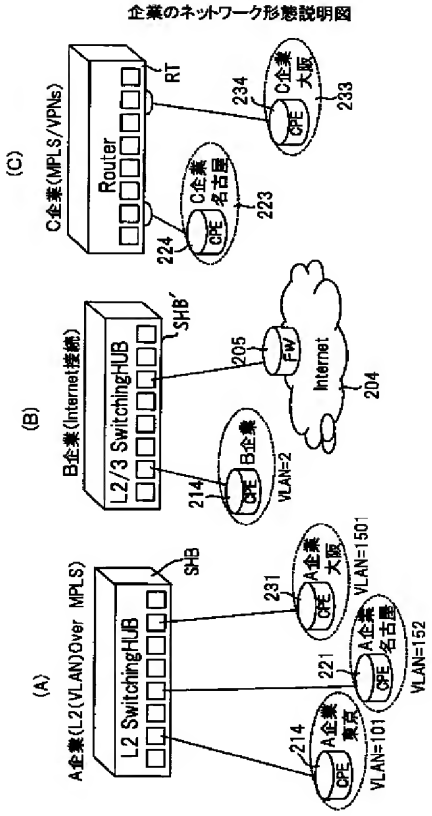
【図6】


MPLSによる企業のネットワーク形態説明図
Internet
204
205
FW
VLAN=2(NoTag)
MPLS網
200
PE
218
IBGP-MP
RouterReflector
212
211
L2
Switch
215
214
217
216
B企業
VLAN=2
A企業
東京
VLAN=101
VLAN Domain東京
201
222
221
A企業
名古屋
VLAN=152
VLAN Domain名古屋
202
224
223
C企業
CPE
232
231
A企業
大阪
VLAN=1501
VLAN Domain名古屋
203
234
233
XXXXXX
■PE:キャリア網でのエッジルータ(VLAN未対応)
■CPE:ユーザのルータ(PEにつながる)

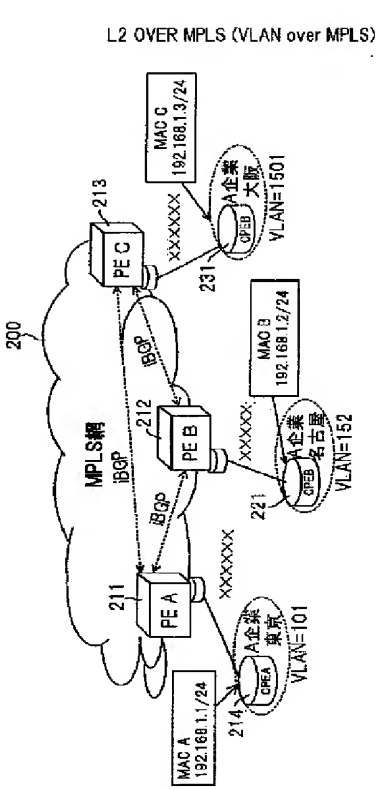
【図19】


複数のスイッチングハブに属するポートをグループ化したVLAN構成例
SHB1
スイッチングハブ
ポート1 VLAN1
ポート2 VLAN2
ポート3 VLAN3
SHB2
スイッチングハブ
ポート1 VLAN1
ポート2 VLAN2
ポート3 VLAN3
SHB3
スイッチングハブ
ポート1 VLAN1
ポート2 VLAN2
ポート3 VLAN3
VLAN1
VLAN2
VLAN3

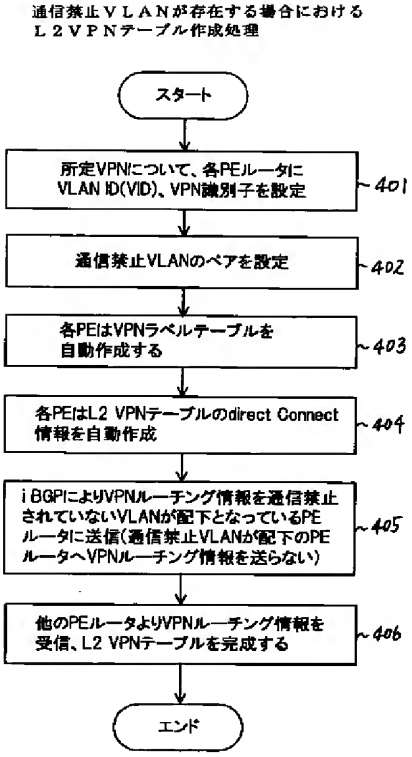
【図7】



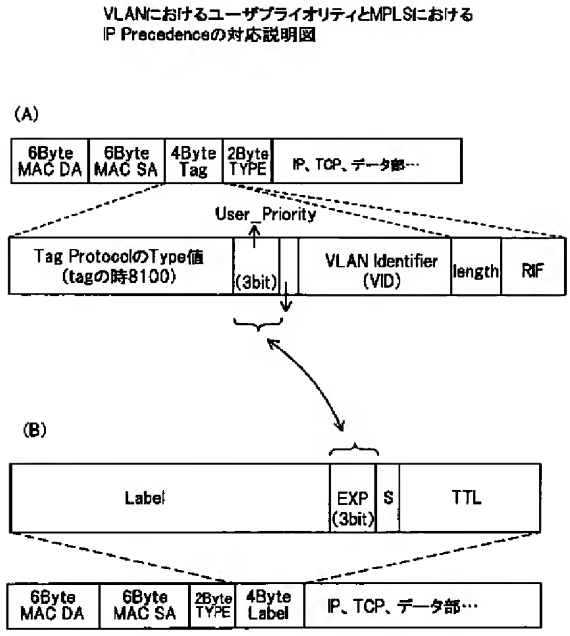
【図8】



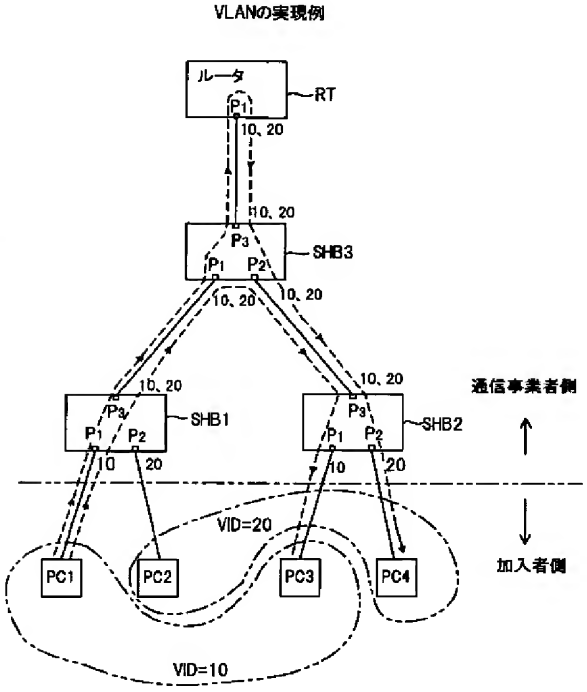
【図16】



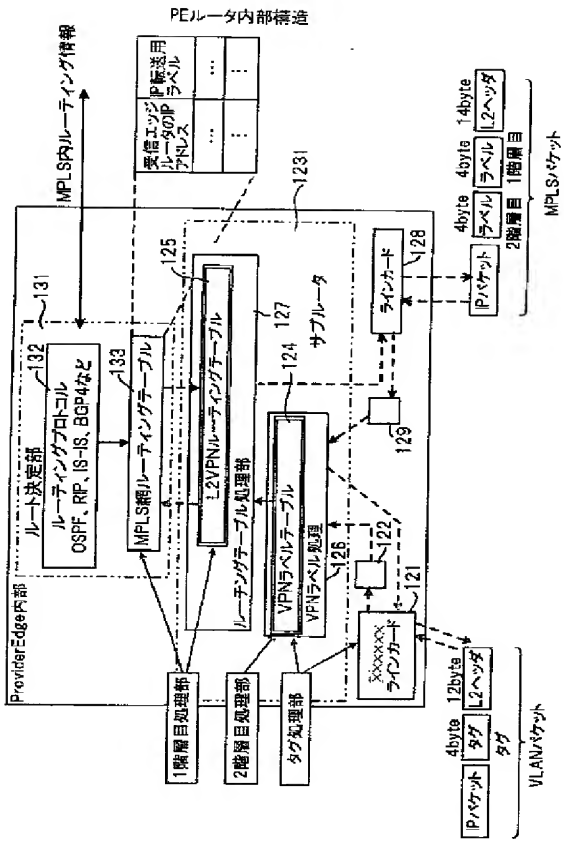
【図17】



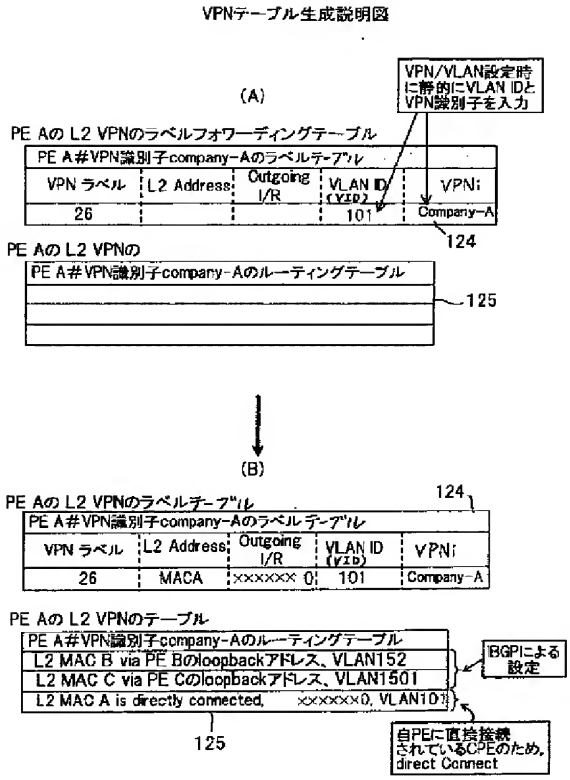
【図21】



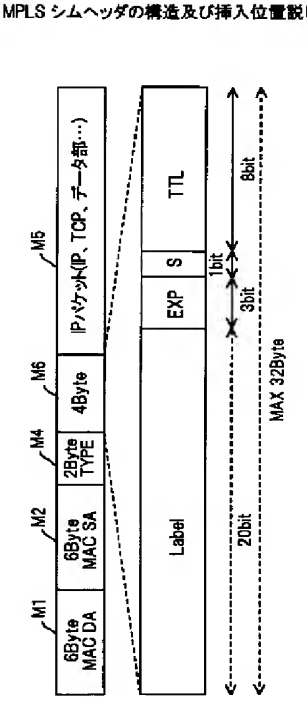
【図９】


PEルータ内部構造
MPLS内ルーティング情報
受信エッジルータのIPアドレス
IP転送用ラベル
131
132
ルート決定部
ルーティングプロトコル
OSPF、RIP、IS-IS、BGP4など
133
MPLS網ルーティングテーブル
125
L2VPNルーティングテーブル
ルーティングテーブル処理部
127
サブルータ
124
VPNラベルテーブル
VPNラベル処理
126
122
121
123
ラインカード
128
129
4byte ラベル
4byte ラベル
4byte 14byte L2ヘッダ
IPパケット
2階層目 1階層目
MPLSパケット
Provider Edge内部
1階層目処理部
2階層目処理部
タグ処理部
Xxxxxx ラインカード
4byte タグ
12byte L2ヘッダ
IPパケット
タグ
VLANパケット

【図１０】


VPNテーブル生成説明図
(A)
VPN/VLAN設定時に静的にVLAN IDとVPN識別子を入力
PE AのL2 VPNのラベルフォワーディングテーブル
PE A#VPN識別子company-Aのラベルテーブル
VPN ラベル
L2 Address
Outgoing I/R
VLAN ID (VID)
VPNi
26
101
Company-A
124
PE AのL2 VPNの
PE A#VPN識別子company-Aのルーティングテーブル
125
(B)
PE AのL2 VPNのラベルテーブル
124
PE A#VPN識別子company-Aのラベルテーブル
VPN ラベル
L2 Address
Outgoing I/R
VLAN ID (VID)
VPNi
26
MACA
xxxxxx 0
101
Company-A
PE AのL2 VPNのテーブル
PE A#VPN識別子company-Aのルーティングテーブル
L2 MAC B via PE Bのloopbackアドレス、VLAN152
L2 MAC C via PE Cのloopbackアドレス、VLAN1501
L2 MAC A is directly connected, xxxxxx0, VLAN10
BGPによる設定
125
自PEに直接接続されているCPEのため、direct Connect

【図２４】


MPLS シムヘッダの構造及び挿入位置説明図
M5
IPパケット(IP、TCP、データ部…)
M6
4Byte
M4
2Byte TYPE
M2
6Byte MAC SA
M1
6Byte MAC DA
TTL
S
EXP
Label
1bit
3bit
8bit
20bit
MAX 32Byte

【図11】

各PEにおける企業のVPNテーブル説明図

(a)PEAにおけるA企業のVPNテーブル

#A企業のL2 VPNラベルテーブル

VPN ラベル	Outgoingl/F	MAC	VID	VPNi
26	×××××××	MAC A	101	ComanyA

#A企業のL2VPNルーチングテーブル

L2	MAC B	PE Bのloopbackアドレス、VLAN152
L2	MAC C	PE Cのloopbackアドレス、VLAN1501
L2	MAC A	directly connected, ××××××, VLAN101

(b)PEBにおけるB企業のVPNテーブル

#A企業のL2 VPNラベルテーブル

NPN ラベル	Outgoingl/F	MAC	VID	VPNi
26	×××××××	MAC B	152	CompanyA

#A企業のL2VPNテーブル

L2	MAC B	directly connected, ××××××, VLAN152
L2	MAC C	PE Cのloopbackアドレス、VLAN1501
L2	MAC A	PE Aのloopbackアドレス、VLAN101

(c)PECにおけるC企業のVPNテーブル

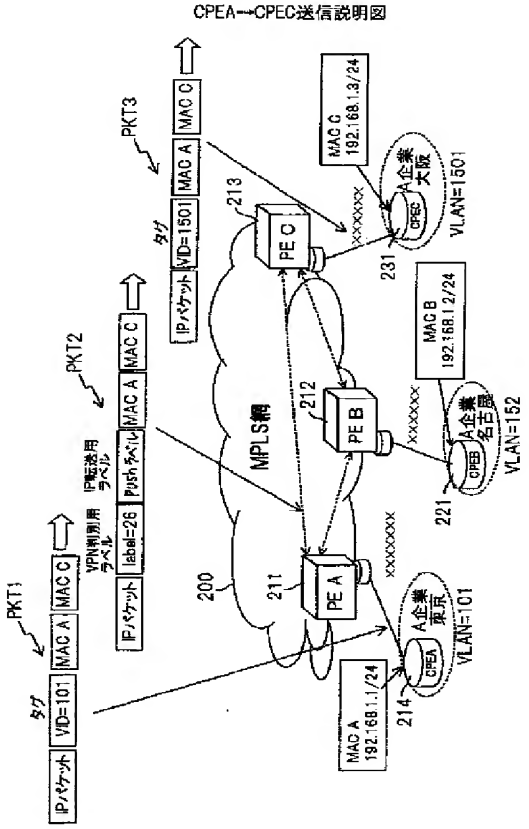
#A企業のL2 VPNラベルテーブル

VPN ラベル	Outgoingl/F	MAC	VID	VPNi
26	×××××××	MAC C	1501	CompanyA

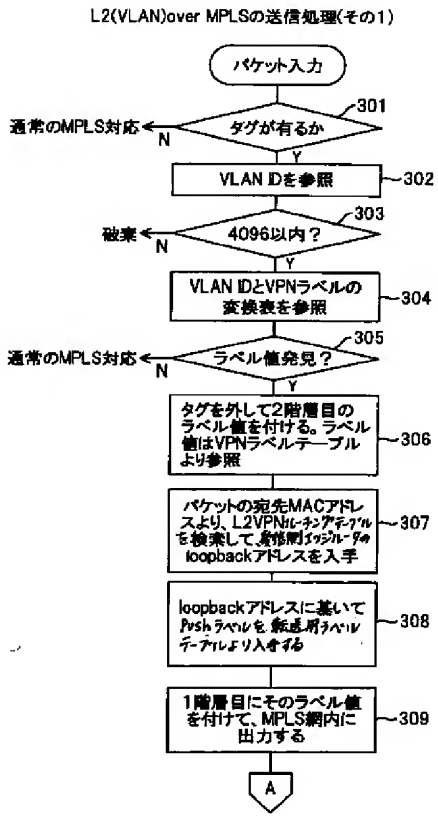
#A企業のL2VPNテーブル

L2	MAC B	PE Bのloopbackアドレス、VLAN152
L2	MAC C	directly connected, ××××××, VLAN1501
L2	MAC A	PE Aのloopbackアドレス、VLAN101

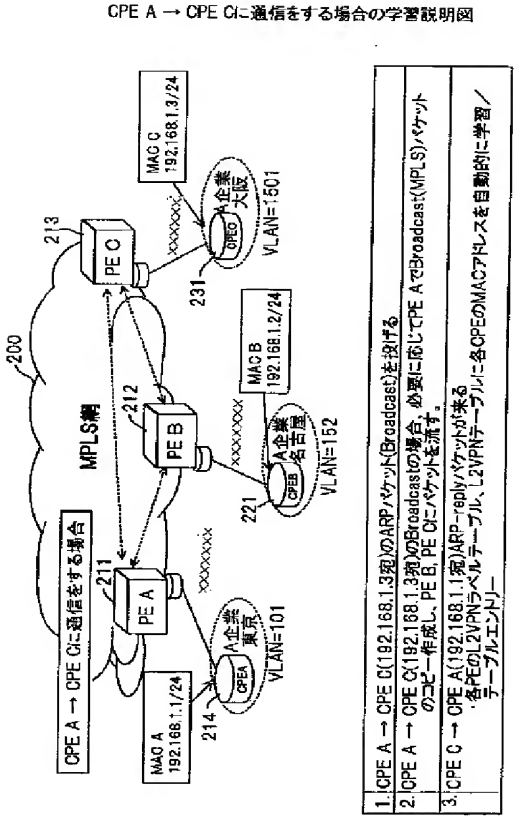
【図12】



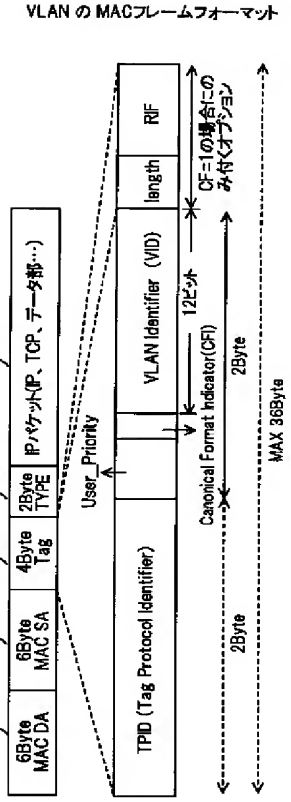
【図13】


L2(VLAN)over MPLSの送信処理(その1)
パケット入力
301
タグが有るか
通常のMPLS対応
N
Y
VLAN IDを参照
302
303
破棄
4096以内？
VLAN IDとVPNラベルの変換表を参照
304
305
ラベル値発見？
タグを外して2階層目のラベル値を付ける。ラベル値はVPNラベルテーブルより参照
306
パケットの宛先MACアドレスより、L2VPNルーティングテーブルを検索して、対向側エッジルータのloopbackアドレスを入手
307
loopbackアドレスに基いてPushするラベルを転送用ラベルテーブルより入手する
308
1階層目にそのラベル値を付けて、MPLS網内に出力する
309
A

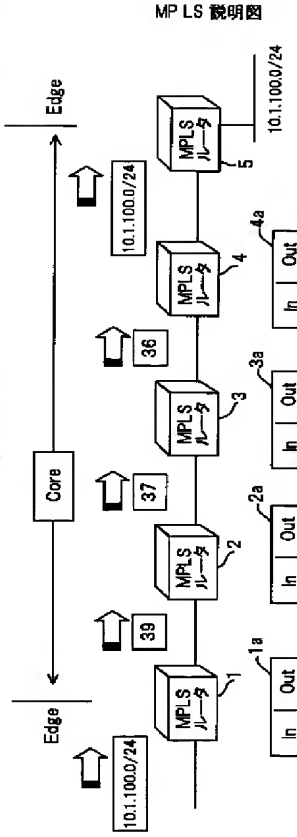
【図15】


CPE A → CPE Cに通信をする場合の学習説明図
MAC C 192.168.1.3/24
MAC B 192.168.1.2/24
MAC A 192.168.1.1/24
PE C
PE B
PE A
MPLS網
200
213
212
211
214
231
221
CPE A → CPE Cに通信をする場合
A企業 大阪
CPEC
VLAN=1501
A企業 名古屋
CPEB
VLAN=152
A企業 東京
CPEA
VLAN=101
1. CPE A → CPE C(192.168.1.3宛)のARPパケット(Broadcast)を投げる
2. CPE A → CPE C(192.168.1.3宛)のBroadcastの場合、必要に応じてCPE Aでbroadcast(MPLS)パケットのコピー作成し、PE B, PE Cにパケットを流す。
3. CPE C → CPE A(192.168.1.1宛)ARP−replyパケットが来る
・各PEのL2VPNラベルテーブル、L2VPNテーブルに各CPEのMACアドレスを自動的に学習／テーブルエントリー

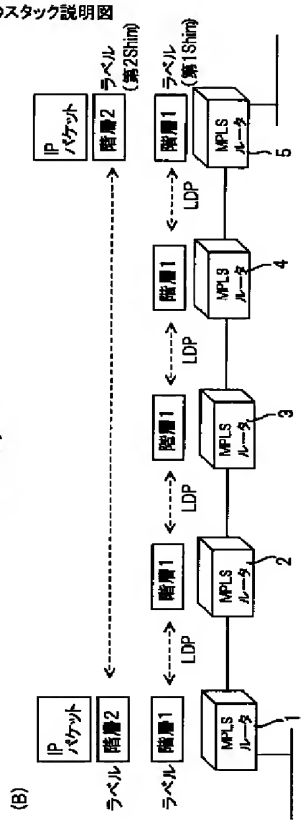
【図20】


VLAN の MACフレームフォーマット
M1
6Byte MAC DA
M2
6Byte MAC SA
M3
4Byte Tag
M4
2Byte TYPE
M5
IPパケット(IP、TCP、データ部…)
User_Priority
TPID (Tag Protocol Identifier)
VLAN Identifier (VID)
12ビット
Canonical Format Indicator(CFI)
length
RIF
CF=1の場合にのみ付くオプション
2Byte
2Byte
MAX 36Byte

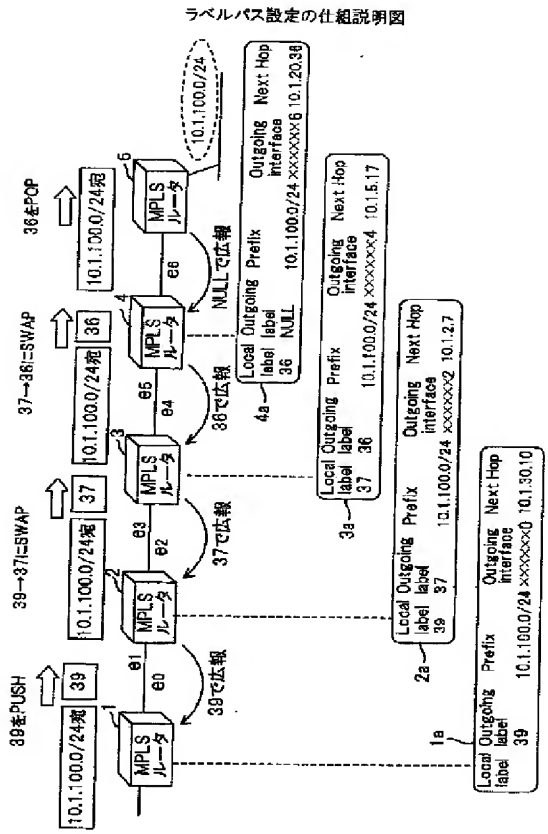
【図22】


MP LS 説明図
Edge
Core
Edge
10.1.100.0/24
10.1.100.0/24
MPLS ルータ
1
2
3
4
5
39
37
36
1a
2a
3a
4a
In
Out
Push Label
Label swapping
Pop Label
M1
6Byte MAC DA
M2
6Byte MAC SA
M4
2Byte TYPE
M6
4Byte 第1シム ヘッダ
M7
4Byte 第2シム ヘッダ
M5
IPパケット(IP、TCP、データ部…)
(A)

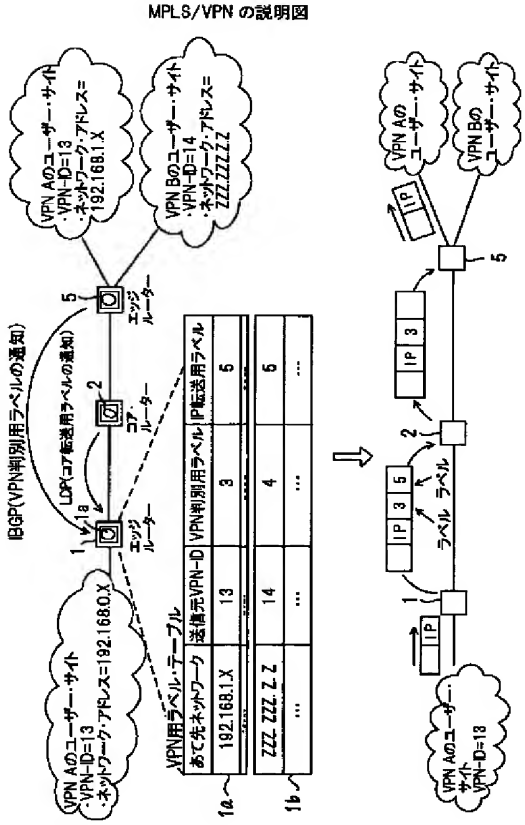
【図25】


シムヘッダのスタック説明図
Label
EXP
S
TTL
16bit
3bit
8bit
20bit
MAX 32Byte
IP パケット
階層2
ラベル (第2Shim)
ラベル (第1Shim)
階層1
LDP
MPLS ルータ
1
2
3
4
5
(B)

【図23】


ラベルパス設定の仕組説明図
39をPUSH
39→37にSWAP
37→36にSWAP
36をPOP
10.1.100.0/24宛
39
37
36
MPLS ルータ
e0
e1
e2
e3
e4
e5
e6
39で広報
37で広報
38で広報
NULLで広報
10.1.100.0/24
Local label
Outgoing label
Prefix
Outgoing interface
Next Hop
1a
2a
3a
4a
10.1.30.10
10.1.2.7
10.1.5.17
10.1.20.38

【図26】


MPLS/VPN の説明図
VPN Aのユーザー・サイト
・VPN-ID=13
・ネットワーク・アドレス=192.168.1.X
VPN Bのユーザー・サイト
・VPN-ID=14
・ネットワーク・アドレス=ZZZ.ZZZ.Z.Z
BGP(VPN別用ラベルの通知)
LDP(コア転送用ラベルの通知)
エッジルーター
コアルーター
VPN用ラベル・テーブル
あて先ネットワーク
送信元VPN-ID
VPN別用ラベル
IP転送用ラベル
192.168.1.X
13
3
5
ZZZ.ZZZ.Z.Z
14
4
6
IP
ラベル
VPN Aのユーザー・サイト
VPN-ID=13
VPN Aのユーザー・サイト
VPN Bのユーザー・サイト

【図27】

MPLS/VPNsの説明図